Chartered Accountants of Canada

Comptables agréés du Canada

Exposure Draft – February 1, 1999

AICPA/CICA

WebTrust℠ Principles and Criteria

for

Business-to-Consumer Electronic Commerce

Version 1.1

Comments should be sent by March 12, 1999, to Mr. Anthony Pugliese (apugliese@aicpa.org) American Institute of Certified Public Accountants, 1211 Avenue of the Americas, New York, New York 10036, USA or to Mr. Bryan Walker (bryan.walker@cica.ca), Canadian Institute of Chartered Accountants, 277 Wellington Street West, Toronto, Ontario M5V 3H2 Canada

Preface

The Internet provides consumers with a new means for obtaining useful information and for purchasing goods and services. Although this form of electronic commerce has undergone rapid growth, particularly through the use of the World Wide Web (the "Web"), its growth has been inhibited by consumer fears and concerns about the risks, both real and perceived, of doing business electronically.

In response to these fears and concerns and to increase consumer confidence in this new electronic marketplace, the public accounting profession has developed and is promoting this set of principles and criteria for business-to-consumer electronic commerce, referred to as the *WebTrust*℠ Principles and Criteria, and the related *WebTrust* seal of assurance, also referred to as CPA *WebTrust*℠ and CA *WebTrust*™. Public accounting firms and practitioners, who have a *WebTrust* business license from the American Institute of Certified Public Accountants (AICPA), Canadian Institute of Chartered Accountants (CICA), or other authorized national institutes ("practitioners"), can provide assurance services to evaluate and test whether a particular Web site meets these principles and criteria. The *WebTrust* seal of assurance is a symbolic representation of a practitioner's unqualified report. It also indicates to customers that they need to click to see the practitioner's report**.** This seal can be displayed on the entity's Web site together with links to the practitioner's report and other relevant information.

This is version 1.1 of the *WebTrust* Principles and Criteria. Its focus is business-to-consumer transactions. The principal features of Version 1.1: (a) expand the illustrative business practice disclosures and illustrative controls of transaction integrity and information protection principles to include online banking and securities trading entities, (b) address year 2000 risks and modify the auditors' report accordingly, and (c) provide for direct reporting in accordance with recently promulgated AICPA Statement on Standards for Attestation Standards No. 9**,** *Amendments to Statements on Standards for Attestation Standards Nos. 1, 2 and 3.* We anticipate that future revisions will be needed to update these criteria and related materials. Additional principles and criteria also may be developed to expand the focus to include business-to-business transactions and other aspects of electronic commerce.

The *WebTrust* Principles and Criteria are intended to address user needs and concerns and are designed to benefit users and providers of electronic commerce services. Your input is not only welcome, it is essential to help ensure that these principles and their supporting criteria are kept up-to-date and remain responsive to marketplace needs.

This version of the *WebTrust* Principles and Criteria has been approved for exposure by the AICPA Assurance Services Executive Committee and the CICA Assurance Services Development Board.

Robert L. Bunting, CPA**,** Chairman
AICPA Assurance Services Executive Committee

John W. Beech, CA, Chairman
CICA Assurance Services Development Board

Your comments are welcome and should be sent to Mr. Anthony J. Pugliese (apugliese@aicpa.org) or Mr. Bryan Walker (bryan.walker@cica.ca). Updated versions will be published at the AICPA Web site (http://www.aicpa.org/webtrust/princrit.htm) and at the CICA Web site (http://www.cica.ca).

Table of Contents

Introduction

The public accounting profession has developed the *WebTrust* Principles and Criteria and the related *WebTrust* seal of assurance to assist entities and their customers in assessing the risks of doing business electronically. This document explains electronic commerce, the risks that are addressed by the electronic commerce principles and criteria, and the seal of assurance, and presents the principles and the related measurement criteria.

BACKGROUND

What Is Electronic Commerce?

Electronic commerce involves individuals as well as organizations engaging in a variety of electronic business transactions, without paper documents, using computer and telecommunication networks. These networks can be public, private or a combination of the two. Traditionally, the definition of electronic commerce has focused on Electronic Data Interchange (EDI) as the primary means of conducting business electronically between entities having a pre-established contractual relationship. More recently, however, the definition of electronic commerce has broadened to encompass business conducted over the Internet (specifically the Web) and includes entities not previously known to each other. This is due to the Web's surge in popularity and the acceptance of the Internet as a viable transport mechanism for business information. The use of a public network-based infrastructure like the Internet can reduce costs and "level the playing field" for small and large businesses. This allows companies of all sizes to extend their reach to a broad customer base.

What Are the Risks in Electronic Commerce?

The following are broad areas of risk associated with electronic commerce.

Business Practices

Electronic commerce often involves transactions between strangers. Appearances can be deceiving. How can a consumer know whether an entity that presents a well-constructed Web page will really fill its orders for goods and services as it claims? How can a consumer know whether the entity will allow the return of goods, or whether there are product warranties? The anonymity of electronic commerce and the ease with which the unscrupulous can establish – and abandon – electronic identities make it crucial that people know that those entities with which they are doing business disclose and follow certain business practices. Without such useful information and the assurance that the entity has a history of following such practices, consumers could face an increased risk of loss, fraud, inconvenience, or unsatisfied expectations.

Transaction Integrity

Without proper controls, electronic transactions and documents can be easily changed, lost, duplicated and incorrectly processed. These attributes may cause the integrity of electronic transactions and

documents to be questioned, causing disputes regarding the terms of a transaction and the related billing. Potential participants in electronic commerce may seek assurance that the entity has effective transaction integrity controls and a history of processing its transactions accurately, completely, and promptly, and of billing its customers in accordance with agreed-upon terms.

Information Protection

It is important for consumers to have confidence that they have reached a properly identified Web site and that the entity takes appropriate steps to protect private customer information. Although it is relatively easy to establish a Web site on the Internet, the underlying technology can be complex and can entail a multitude of information protection and related security issues. The confidentiality of sensitive information transmitted over the Internet can be compromised. For example, without the use of basic encryption techniques, consumer credit card numbers can be intercepted and stolen during transmission. Without appropriate firewalls and other security practices, private customer information residing on an entity's electronic commerce computer system can be intentionally or unintentionally provided to third parties not related to the entity's business. Security breaches may also include unauthorized access to corporate networks, Internet/Web servers, and even access to the consumer's Internet connection (for example, his or her home computer). Potential participants in electronic commerce may seek assurance that the entity has effective information protection controls and a history of protecting private customer information.

The Year 2000 Issue

The Year 2000 Issue has had much publicity, but although all entities should be aware of it, responses are varied, with some entities still doing little. The issue is simple to explain; it has arisen because where computerized systems identify the year using two digits only, the digits 00 may be misinterpreted, for example, as 1900 or a special code or an error condition, potentially causing errors or operational failure of computerized systems. In addition, some computerized systems do not properly perform calculations with dates beginning in 1999, because these systems use the digits 99 in date fields to represent something other that the year 1999. It is also important to recognize that the Year 2000 is a leap year and that not all systems recognize February 29, 2000 as a valid date. The Year 2000 Issue may manifest itself before, on or after January 1, 2000 and its effects on financial reporting and operations may range from inconsequential errors to business failure.

It is the responsibility of an entity's management to assess and remediate the effects of the Year 2000 Issue on an entity's systems. This responsibility extends beyond systems that produce financial information. It encompasses all systems, including those that are part of the entity's operational activities, such as safety, environment, production, machine control, service, and security activities. Management also is responsible for considering the effect that other entities' noncompliant systems may have on its operations and financial information system. The board of directors (or others with equivalent responsibility) has a responsibility to oversee the activities of management to ensure that the Year 2000 Issue is receiving appropriate attention from management.

It is important to recognize that it is not, and will not, be possible for any entity to represent that it has achieved complete Year 2000 compliance and guarantee its remediation. The problem is simply too complex for such a claim to have legitimacy. The nature and complexity of the issue means that efforts

to deal with Year 2000 problems are effectively risk mitigation. Accordingly, no assurance regarding Year 2000 compliance is provided as part of the *WebTrust* service.

THE WEBTRUST SEAL OF ASSURANCE

The Web has captured the attention of businesses and consumers, causing the number and types of electronic transactions to grow rapidly. Nevertheless, many feel that electronic commerce will not reach its full potential until customers perceive that the risks of doing business electronically have been reduced to an acceptable level. Customers may have legitimate concerns about transaction integrity, control, authorization, confidentiality and anonymity. In the faceless world of electronic commerce, participants need the assurance of an objective third party. This assurance can be provided by an independent and objective certified public accountant (CPA) or chartered accountant (CA) and demonstrated through the display of a secured *WebTrust* seal.

The *WebTrust* seal of assurance symbolizes to potential customers that a CPA or CA has evaluated the Web site's business practices and controls to determine whether they are in conformity with the *WebTrust* Principles and Criteria for Business-to-Consumer Electronic Commerce, and has issued a report with an unqualified opinion indicating that such principles are being followed in conformity with the *WebTrust* Criteria. See Appendix A, "Illustrative Examples of Practitioner Reports." These principles and criteria reflect fundamental standards for business practices, transaction integrity, and information protection.

THE CPA AND THE CA AS ASSURANCE PROFESSIONALS

CPAs and CAs are in the business of providing assurance services, the most publicly recognized of which is the audit of financial statements. An audit opinion signed by a CPA or CA is valued because these professionals are experienced in assurance matters and financial accounting subject matter and are recognized for their independence, integrity, discretion, and objectivity. CPAs and CAs also follow comprehensive ethics rules and professional standards in providing their services. However, financial statement assurance is only one of the many types of assurance services that can be provided by a CPA or CA. CPAs and CAs also provide assurance about internal controls and compliance with specified criteria. The business and professional experience, subject matter expertise (electronic commerce information systems security, auditability, and control) and professional characteristics (independence, integrity, discretion, and objectivity) needed for such projects are the same key elements that enable a CPA or CA to comprehensively and objectively assess the risks, controls, and business disclosures associated with electronic commerce.

OBTAINING AND KEEPING THE *WEBTRUST* SEAL OF ASSURANCE

The Assurance Process

The entity's management will make representations or assertions to the practitioner along the following lines:

ABC Company, on its Web site for electronic commerce (at WWW.ABC.COM):

- Disclosed its business practices for electronic commerce transactions and executed transactions in accordance with its disclosed business practices,
- Maintained effective controls to provide reasonable assurance that customers' transactions using electronic commerce were completed and billed as agreed, and
- Maintained effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce was protected from uses not related to ABC's business

  During the period Xxxx xx, 199x through Yyyy yy, 199x in conformity with the AICPA/CICA *WebTrust* Criteria.

For an initial representation, the historical period covered should be at least two months or more as determined by the practitioner. For subsequent representations, the period covered should begin with the end of the prior period to provide continuous representation.

In order to have a basis for such representations, the entity's management should have appropriate internal controls for its electronic commerce transactions. Helpful guidance can be found, for example, in material developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in the US, and the Criteria of Control (CoCo) in Canada. However, for purposes of obtaining the WebTrust seal of assurance the practitioner will only evaluate those elements of internal control that are relevant to processing electronic commerce transactions.

An independent, objective and knowledgeable practitioner will perform tests of these representations under AICPA or CICA professional standards[1] and provide a professional opinion, which adds to the credibility of management's representations.

Obtaining the Seal

To obtain the *WebTrust* seal of assurance, the entity must meet all the *WebTrust* Principles as measured by the *WebTrust* Criteria associated with each of these principles. In addition, the entity must (1) engage a CPA or CA practitioner, who has a *WebTrust* business license from the AICPA, CICA, or other authorized national accounting institute to provide the *WebTrust* service and (2) obtain an unqualified report from such practitioner. A self-assessment questionnaire has been provided as Appendix B to assist the entity's management in forming a basis for their assertions.

Keeping the Seal

Once the seal is obtained, the entity will be able to continue displaying it on its Web site provided:

[1] These services are performed in the United States under the AICPA's Statement on Standards for Attestation Engagements, No 1 (also known as AICPA Professional Standards Section AT100) or in Canada under the CICA's Standards for Assurance Engagements (also known as *CICA Handbook* Section 5025). Practitioners will need the appropriate skills and experience, training in the *WebTrust* service offering, and a *WebTrust* business license from the AICPA, CICA, or other authorized national accounting institute in order to provide the *WebTrust* services to their clients. The practitioner needs to perform an "examination" (audit) level engagement in order to award the *WebTrust* seal. A "review" level engagement is not sufficient.

1. Its assurance practitioner updates his or her assurance examination of the assertion on a regular basis. The interval between such updates will depend on matters such as:
   - The nature and complexity of the entity's operation,
   - The frequency of significant changes to its Web site,
   - The relative effectiveness of the entity's monitoring and change management controls for ensuring continued conformity with the *WebTrust* Criteria as such changes are made, and
   - The practitioner's professional judgment.

   For example, an update will be required more frequently for a financial institution's fast-changing Web site for securities transactions than for an on-line service that sells archival information using a Web site that rarely changes. In no event should the interval between updates exceed 3 months and this interval often may be considerably shorter.

2. During the period between updates, the entity undertakes to inform the practitioner of any significant changes in its business policies, practices, processes, and controls particularly if such changes might affect the entity's ability to continue meeting the *WebTrust* Principles and Criteria, or the manner in which they are met. Such changes may trigger the need for an assurance update or, in some cases, removal of the seal until an update examination by the practitioner can be made. If the practitioner becomes aware of such a change in circumstances, he or she would determine whether an update examination would need to be performed and whether the seal would need to be removed until the update examination was completed and the updated auditor's report is issued.

The Seal Management Process

The *WebTrust* seal of assurance will be managed using a trusted-third-party service organization (the "seal manager") along the following lines:

- The entity will need to apply for and receive a special Class 3 Certificate (the "WebTrust digital certificate") from the seal manager.
- If the entity receives an unqualified report, the practitioner will notify the seal manager that the seal can be displayed on the Web site of the entity with a particular digital identification and will provide an expiration date.
- The practitioner or seal manager also will provide an applet (a type of computer program used on the Web) to the entity, which instructs a Web page to communicate with the seal manager and, if authorized, display the seal and related hot links to the practitioner's report and other relevant information. The seal manager will also provide a special *WebTrust* digital certificate to the entity.
- If, for an appropriate reason, the practitioner determines that the seal should be removed from the entity's Web site, he or she will notify the entity and request that the seal and the related practitioner's report be removed from the Web site. The practitioner also will send a seal display authorization removal notification to the seal manager. This will electronically revoke the seal and prevent it from being displayed by the entity.
- Unless an update notification is received, (1) the authorization to display the seal will expire, (2) the Web site will be requested to remove the seal and the practitioner's report and (3) the seal manager will remove the entity's seal display authorization as of the expiration date.

Seal Authentication

To verify whether the seal displayed on a Web site is authentic, the customer can click on the seal and a graphic display, which looks like a certificate, will appear. This display will provide the customer with directions on how to view the special *WebTrust* digital certificate issued by the seal manager using the browser. This digital certificate provides the customer with evidence that the *WebTrust* seal is valid. The digital certificate will indicate (1) that it was issued by VeriSign, Inc., (2) that it was issued as a result of a WebTrust examination, (3) who it was issued to, and (4) where the company awarded the seal is located. Without this digital certificate, the *WebTrust* seal should *not* be considered valid.

WebTrust Principles & Criteria[2]

Although electronic commerce can be conducted through a number of means, including electronic bulletin boards and formalized EDI arrangements, the focus of this version of the criteria is on business-to-consumer electronic commerce conducted through the Web.

The following principles have been developed with the consumer-user in mind and, as a result, are intended to be practical and somewhat non-technical in nature.

THE *WEBTRUST* PRINCIPLES

Business Practices Disclosure

> *The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.*

To enhance customer confidence in electronic commerce, it is important that the customer is informed about the entity's business practices for electronic commerce transactions. As a result, it is important that the entity properly discloses its business practices for dealing with such matters as orders and any subsequent returns and warranty claims and that the entity actually follows such practices. This principle relates to the electronic commerce transaction processes that the entity uses and does not include any representation as to the quality of its goods or services nor their suitability for any customer's intended purpose (as such matters are outside the scope of the *WebTrust* Principles and Criteria).

Transaction Integrity

> *The entity maintains effective controls to provide reasonable assurance that customers' transactions using electronic commerce are completed and billed as agreed.*

These controls and practices address matters such as: (1) transaction validation; (2) the accuracy, completeness, and timeliness of transaction processing and related billings; (3) the disclosure of terms and billing elements and, if applicable, electronic settlement; and (4) appropriate transaction

[2] These criteria meet the definition of "criteria established by a recognized body" described in the third General Standard for attestation engagements in the US (see AT 100.11) and in the standards for assurance engagements in Canada (see CICA Handbook paragraph 5025.41).

identification. These matters are important to promote confidence in electronic commerce.

Information Protection

> *The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce is protected from uses not related to the entity's business.*

These controls and practices address privacy and security matters such as encryption or other protection of private customer information (such as credit card numbers and personal and financial information) transmitted to the entity over the Internet, protection of such information once it reaches the entity and requesting permission of customers to use their information for purposes other than those related to the entity's business, and for obtaining customer permission before storing, altering, or copying information on the customer's computer. Consumer concern about the safeguarding of private information traditionally has been one of the most significant deterrents to undertaking electronic commerce transactions.

THE *WEBTRUST* CRITERIA

In order to provide more specific guidance on meeting the *WebTrust* Principles, the *WebTrust* Criteria have been developed. These provide a basis against which an entity can make a self assessment of its conformity with the criteria and provide a consistent set of measurement criteria for practitioners to use in testing and evaluating Web sites.

A four-column presentation has been used to present and discuss the criteria. The first column presents the criteria - the attributes that the entity must meet to be able to demonstrate that they have achieved the principle. The second through fourth columns provide illustrative disclosures and controls for retail goods and other non-financial services, online banking and online securities trading, respectively. These are examples of disclosures the entity might make and controls that the entity might have in place to conform to the criteria. Alternative and additional disclosures and controls also can be used.

The entity must be able to demonstrate over a period of time (at least 2 months or more) that (1) it executed transactions in accordance with the business practices it discloses for electronic commerce transactions, (2) its controls operated effectively, (3) it maintains a control environment that is conducive to reliable business practice disclosures and effective controls, and (4) it maintains monitoring procedures to ensure that such business practices remain current and such controls remain effective. These concepts are an integral part of the *WebTrust* Criteria.

Business Practices Disclosure – The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.			
Criteria	**Illustrative Disclosures for Retail Goods and Other Non-financial Services**	**Illustrative Disclosures for Online Banking**	**Illustrative Disclosures for Online Securities Trading**
Description of goods and/or services 1. The entity discloses descriptive information about the nature of the goods that will be shipped or the services that will be provided, including, but not limited to, the following:			
• Condition of goods (i.e., whether they are new, used, or reconditioned).	• You can purchase new and used books on our site; used books are clearly labeled as such.		
• Description of services (or service contract).		• Our Internet Services are as follows: – 24-hour access to your bank accounts. – Pay bills including heat, water, phone, cable TV, credit and department store cards, taxes and gas. – Transfer funds between your accounts.	• ABC Trading Inc. offers a wide range of trading account types, including Cash Accounts, Margin Accounts, Options Accounts and Short Sell Accounts. All have competitive rates so your money earns interest even when it's idle.

Business Practices Disclosure – The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.			
Criteria	**Illustrative Disclosures for Retail Goods and Other Non-financial Services**	**Illustrative Disclosures for Online Banking**	**Illustrative Disclosures for Online Securities Trading**
		– Check account balances on your bank accounts. – Keep track of the entries that have gone through your accounts. – Make payments or draw down on your Credit Line. – Obtain balances and make payments on most loans. • You may access your checking account, savings account, money market accounts, home equity line of credit through our on-line service.	• Our Internet Services are as follows: – US & Canadian Equities – Buy or sell securities listed on the AMEX, NASDAQ, NYSE, TSE, ME, VSE, ASE. – Options Trading - Buy puts and calls or write (sell) covered puts and calls on any exchange in the US or Canada. – Short Selling - Short selling involves us borrowing the stock on the investor's behalf to cover the short-sale initially. The short sale of securities involves high degree of risk and therefore may not be suitable for every investor. – Foreign Equities - Trade extensively in most foreign exchanges around the world, including: Hong Kong, Shanghai, Shenzhen, Jakarta, Thailand, Kuala

Business Practices Disclosure – The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.			
Criteria	**Illustrative Disclosures for Retail Goods and Other Non-financial Services**	**Illustrative Disclosures for Online Banking**	**Illustrative Disclosures for Online Securities Trading**
			Lumpur, London, Tokyo, Paris, Frankfurt, Geneva, Sydney, Johannesburg, Zurich, Singapore, Manila and many more. – Mutual Funds - Over 1000 North American Mutual Funds are available. • You can view your investment account, send trade requests, see the status of your trades and the value of your portfolio 24 hours a day, every day.
• Sources of information (i.e., where it was obtained and how it was compiled).	• This report was compiled by us based on scientific evidence from research done at ten universities, which are listed in the report. An analysis prepared by our scientists also is included. Further reproduction or dissemination of all or portions of this report without our written	• The Federal Reserve Bank provides prime lending rate information. Bond rating information is provided by Standard and Poors.	• To provide you with best-price execution, ABC Trading Inc. uses a sophisticated computerized routing system. Orders are directed to the best market based on price and liquidity.

Business Practices Disclosure – The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.			
Criteria	**Illustrative Disclosures for Retail Goods and Other Non-financial Services**	**Illustrative Disclosures for Online Banking**	**Illustrative Disclosures for Online Securities Trading**
	permission is prohibited under copyright law.		
Terms & conditions 2. The entity discloses the terms and conditions by which it conducts its electronic commerce transactions including, but not limited to, the following:			
• Time frame for completion of transactions (transaction means fulfillment of orders where goods are being sold and delivery of service where a service is being provided).	• Our policy is to ship orders within one week of receipt of a customer-approved order. Our experience is that over 90% of our orders are shipped within 48 hours, the remainder is shipped within one week.	• A transfer of funds before 5PM (Pacific Time) on a business day is posted to your account the same day. All transfers completed after 5PM (Pacific Time) on a business day or on a Saturday, Sunday or banking holiday will be posted on the next business day.	• Market orders placed when the markets are open are typically executed and confirmed in a matter of seconds. For limit orders placed during market hours, our best market determination module will determine where the order gets placed. If the market is closed, your order is transmitted to the exchange before the start of the next trading day.

Business Practices Disclosure – The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.			
Criteria	**Illustrative Disclosures for Retail Goods and Other Non-financial Services**	**Illustrative Disclosures for Online Banking**	**Illustrative Disclosures for Online Securities Trading**
			• The real-time status of your order is provided on our web site. In addition, if you have provided us with your e-mail address, you can choose to be notified by e-mail when your order is filled. You will also receive written confirmation of the trade in the mail. • We process your order with the same efficiency as an institutional order, with all the trade execution resources of ABC Trading Inc. • You can enter an order at any time, 7 days a week, 24 hours a day, through the web or through our automated telephone system. If the market is closed when you place your order, it will be reflected at market open on the next trading day. • You will be notified within

Business Practices Disclosure – The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.			
Criteria	**Illustrative Disclosures for Retail Goods and Other Non-financial Services**	**Illustrative Disclosures for Online Banking**	**Illustrative Disclosures for Online Securities Trading**
			five (5) business days prior to expiration of their sell order.
• Time frame and process for informing customers of exceptions to normal processing of orders or service requests	• We will notify you by e-mail within 24 hours if we cannot fulfill your order as specified at the time you placed it and will provide you the option of canceling the order without further obligation. You will not be billed until the order is shipped.	• In the unlikely event we are unable to process your transaction, we will notify you within one hour by e-mail and/or telephone.	• The real-time status of your order is provided on our Web site. In addition, if you have provided us with your e-mail address, you can choose to be notified by e-mail when your order is filled. If, for whatever reason, your order cannot be fulfilled, the status of your order will show an error (Status="ERR") and notify you immediately by e-mail if you have provided us with your e-mail address.
• Normal method of delivery of goods or services, including customer options, where applicable.	• You have the option of downloading the requested information now or we will send it to you on CD-ROM by UPS 2-day or Federal Express overnight delivery.	• In order to sign-in and perform on-line financial transactions, you must use a browser that supports 128 bit encryption.	• In order to sign-in and perform on-line financial transactions, you must use a browser that supports 128 bit encryption.

Business Practices Disclosure – The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.			
Criteria	**Illustrative Disclosures for Retail Goods and Other Non-financial Services**	**Illustrative Disclosures for Online Banking**	**Illustrative Disclosures for Online Securities Trading**
• Payment terms, including customer options, if any.	• Your credit card will be charged at the time of shipment or you can send us a check or money order.	• All bill payments will be withdrawn from the account on the day the payment is scheduled to be sent to the payee whether these payments are made electronically or by check.	• To open an account at ABC Trading, Inc., a minimum of $500 equity is required. This initial deposit can be made with your personal check, securities or any combination of the two. All subsequent equity transferred into your account can be made by a check payment, electronic transfer of funds from your banking account, or by transferring your assets from another broker.
• Electronic settlement practices and related charges to customers.	• Your bank account will be charged $12.95 monthly for our service fee.	• Your account will be immediately debited $30 for each stop payment order requested.	• All stock transactions are settled three day after the trade and option trades are settled one day after the trade.. You will be charged a commission of $20 per trade regardless of the size of your transaction.
• How customers may cancel recurring	• To cancel your monthly service fee, send us an e-	• We will charge you monthly fee of $5 once you sign-up	• There are no monthly or recurring fees associated

Business Practices Disclosure – The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.			
Criteria	**Illustrative Disclosures for Retail Goods and Other Non-financial Services**	**Illustrative Disclosures for Online Banking**	**Illustrative Disclosures for Online Securities Trading**
charges, if any.	mail at Subscriber@ABC.COM or call us at 800-555-1212. Be sure to include your account number.	for online banking. Contact our Customer Service Department at any time should you want to cancel online banking services.	with your account.
• Product return policies and/or limited liability, where applicable.	• Purchases can be returned for a full refund within 30 days of receipt of shipment. Call our 800 number or E-mail us for a Return Authorization Number, which should be written clearly on the outside of the return package.	• If your online password has been compromised and you tell us within two business days after you learn of the loss or theft, your losses are limited to $100 if someone used your online password without your permission. If you do not tell us within two business days after you learn of the loss or theft your losses are limited to $1,000. • If your statement shows withdrawals, transfers or purchases that you did not authorize and you do not notify us within 60 days after the online statement was sent to you, you may not recover any money lost	• The Securities Investors Protection Corporation (SIPC) currently protects the assets in each account up to $500,000, of which no more than $100,000, may be in cash. This protection does not cover fluctuations in the market value of your investments.

Business Practices Disclosure – The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.			
Criteria	**Illustrative Disclosures for Retail Goods and Other Non-financial Services**	**Illustrative Disclosures for Online Banking**	**Illustrative Disclosures for Online Securities Trading**
		after the 60 day period.	
Customer support & service 3. The entity discloses on its Web site (and/or in information provided with the product) where customers can obtain warranty, repair service, and support related to the goods and services purchased on its Web site.	• Warranty and other service can be obtained at any one of our 249 worldwide locations that are listed on this Web site. A list of these locations also is included with all of our products. • For service and other information, contact one of our customer service representatives at 800-555-1212 between 7:00a.m. and 8:00p.m. (Central Standard Time) or you can write to us as follows: Customer Service Department ABC Company 1234 Anystreet Anytown, Illinois 60000 or	• For service and other information, such as your specific rights and responsibilities and for the applicable laws and regulations that govern your transaction send us an e-mail at OnlineServicie@bank.com or call our Customer Service representatives at 1-800-666-8787.	• .Feel free to contact our Customer Service via email, telephone, or regular mail 24-hours a day regarding your specific rights and responsibilities and for the applicable laws and regulations which govern your transaction: – To contact ABC Trading Inc. via electronic mail: Send your message to Customer Service at service@abctrading.com. Email messages sent during market hours are responded to on a timely basis by dedicated online Customer Service representatives. – To contact ABC Trading Inc. via telephone: dial 800-555-1212 between 7:00a.m. and 8:00p.m. (Central

Business Practices Disclosure – The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.			
Criteria	**Illustrative Disclosures for Retail Goods and Other Non-financial Services**	**Illustrative Disclosures for Online Banking**	**Illustrative Disclosures for Online Securities Trading**
	CustServ@ABC.COM		Standard Time) or You can write to us as follows: Customer Service Department ABC Trading Inc. 1234 Anystreet Anytown, Illinois 60000
Customer communications 4. The entity discloses information to enable customers to file claims, ask questions and register complaints, including, but not limited to, the following: • Street address (not a post office box or E-mail address). • Telephone number (a number to reach an employee on a reasonably timely basis and not only a voice mail system or message	• If you wish to file a claim or have questions or complaints about our products, you can call one of our customer service representatives at 800-555-1212 between 7:00a.m. and 8:00p.m. (Central Standard Time) or you can write to us as follows: Customer Service Department ABC Company 1234 Anystreet Anytown, Illinois 60000	• In case of errors or if you have questions or complaints about our services, you can call one of our customer service representatives at 800-666-8787 between 7:00a.m. and 8:00p.m. (Central Standard Time) or you can write to us as follows: Customer Service Department ABC Bank 1234 Anystreet Anytown, Illinois 60000	• In case of errors or if you have questions or complaints about our services, you can call one of our customer service representatives at 800-555-1212 between 7:00a.m. and 8:00p.m. (Central Standard Time) or you can write to us as follows: Customer Service Department ABC Trading Inc. 1234 Anystreet Anytown, Illinois 60000

Business Practices Disclosure – The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.			
Criteria	**Illustrative Disclosures for Retail Goods and Other Non-financial Services**	**Illustrative Disclosures for Online Banking**	**Illustrative Disclosures for Online Securities Trading**
machine). • Days and hours of operation. • If there are several offices or branches, the same information for the principal office	or CustServ@ABC.COM	You must notify us no later than 60 days after we have sent you the first paper or online statement on which the problem or error occurred. When contacting us with a request, please have the following information available: – Name, account number, transaction date, description of error or transaction you are unsure about and why you believe it is an error, the dollar amount of the suspected error, and – For a bill payment the checking account number used to pay the bill, payee name, date the payment was authorized, payment amount, reference number, and payee account number for the payment in question.	

Transaction Integrity - The entity maintains effective controls to provide reasonable assurance that customer's transactions using electronic commerce are completed and billed as agreed.			
Criteria	**Illustrative Disclosures for Retail Goods and Non-financial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
Requesting goods and/or services 1. The entity maintains controls to provide reasonable assurance that:			
• Each request or transaction is checked for accuracy and completeness.	• Web scripts contain error checking for invalid inputs. • The entity's computer system automatically checks each order for accuracy and completeness of information before processing.	• Web scripts contain error checking for invalid inputs. • The entity's computer system automatically checks each financial transaction for accuracy and completeness of information before processing.	• Web scripts contain error checking for invalid inputs. • The entity's computer system automatically checks each trade for accuracy and completeness of information before processing.
• Positive acknowledgment is received from the customer before the transaction is processed	• All customer-provided information for the order is displayed to the customer. Customer accepts an order, by clicking "yes", before the order is processed. • Customer receives a confirming e-mail and can correct or cancel order prior to fulfillment	• All financial transactions are displayed to the customer to accept, by clicking "yes", before the transaction is processed.	• All trades are displayed to the customer to accept, by clicking "yes", before the transaction is processed.

Transaction Integrity - The entity maintains effective controls to provide reasonable assurance that customer's transactions using electronic commerce are completed and billed as agreed.			
Criteria	**Illustrative Disclosures for Retail Goods and Non-financial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
Processing requests for goods and/or services 2. The entity maintains controls to provide reasonable assurance that :			
• The correct goods are shipped in the correct quantities in the time frame agreed, or services and information are provided to the customer as requested.	• Packing slips are created from the customer sales order and checked again as order is picked and packed. • Commercial delivery methods are used that reliably meet expected delivery schedules. • Shipping manifests are retained. • Entity retains customer orders or contract information. • Service delivery targets are maintained and actual services provided are monitored against such targets. • The entity uses a "feedback" questionnaire to confirm customer satisfaction with completion	• The entity's computer system has controls (e.g., balancing controls, daily reconciliation controls) to ensure that submitted transactions are processed completely, accurately and in a timely manner.	• We provide real-time status of your order on our Web site. Customers know immediately if their order was processed correctly. • The entity's computer system has controls (e.g., balancing controls, daily reconciliation controls) to ensure that submitted orders are processed completely, accurately and in a timely manner.

Transaction Integrity - The entity maintains effective controls to provide reasonable assurance that customer's transactions using electronic commerce are completed and billed as agreed.			
Criteria	**Illustrative Disclosures for Retail Goods and Non-financial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
	of service or delivery of information to the customer.		
• Transaction exceptions are promptly communicated to the customer.	• Computerized backorder records are maintained and are designed to notify customers of backorders within 24 hours. Customers are given the option to cancel a backorder or have an alternate item delivered.	• The entity's staff investigates all rejected transactions and escalates unresolved problems to the customer services manager. Customers are notified via e-mail or telephone of potential problems related to online transactions.	• The entity's staff investigates all rejected transactions and escalates unresolved problems to the customer services manager. Customers are notified via e-mail or telephone of potential problems related to online transactions.
Processing bill/payment 3. The entity maintains controls to provide reasonable assurance that:			
• Sales prices and all other costs/fees are displayed for the customer before processing the transaction.	• Customer has the option of printing, before order is processed, an "order confirmation" on line for future verification with payment records (such as credit card statement) detailing all information of the order (such as item(s) ordered, sales prices, costs, sales taxes, shipping	• All financial services fees are displayed on the Web site describing the financial services and the fee options available to the customer. • Each fee option for financial services describes fully the fees (transaction fee, monthly fee, etc.) including any transaction limits in amount and	• All fees (fixed and transaction based) are displayed on the Web site describing the service and the fee options to the customer.

Transaction Integrity - The entity maintains effective controls to provide reasonable assurance that customer's transactions using electronic commerce are completed and billed as agreed.			
Criteria	**Illustrative Disclosures for Retail Goods and Non-financial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
	charges, etc.). • All costs, including taxes and shipping, are displayed to the customer. Customer accepts an order, by clicking "yes", before the order is processed.	number placed on the customer. • All deposit and loan interest rates are displayed to the customer. • All foreign exchange rates are displayed to the customer before performing a transaction involving foreign currency. • The transaction details (e.g., amount, account numbers, bill payment vendor, foreign currency rate, interest rate, transaction fee) are displayed before the customer accepts the transaction. Customer accepts transaction, by clicking "yes", before the transaction is processed.	
• Transactions are billed and electronically settled as agreed.	• Billing and settlement experiences are monitored on a daily basis against policy disclosed at Web site. • Total costs and the expected shipping and billing dates	• A transfer of funds before 5PM (PST) on a business day is posted to your account the same day. All transfers completed after 5PM (PST) on a business day or on a Saturday,	• All trades are settled from your cash account. Market orders placed when the markets are open are typically executed and confirmed in a matter of seconds. For limit orders

Transaction Integrity - The entity maintains effective controls to provide reasonable assurance that customer's transactions using electronic commerce are completed and billed as agreed.			
Criteria	**Illustrative Disclosures for Retail Goods and Non-financial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
	are displayed for the customer before the customer accepts the order.	Sunday or banking holiday will be posted on the next business day. • All bill payments will be withdrawn from the account on the day the payment is scheduled to be sent to the payee whether these payments are made electronically or by check. • Standard procedures exist for establishing the vendor bill payment process and the authorized vendor list.	placed during market hours, our best market determination module will determine where the order gets placed. If the market is closed, your order is transmitted to the exchange before the start of the next trading day.
• Billing or settlement errors are promptly corrected.	• Billing or settlement errors are followed up and corrected within 24 hours of reporting by the customer.	• Posting errors are followed up and corrected within 24 hours of reporting by the customer.	• Posting errors are followed up and corrected within 24 hours of reporting by the customer.
Transaction history 4. The entity maintains controls that allow for subsequent follow-up of transactions.	• The company maintains a transaction history for each order. • Each order has a unique identifier that can be used to access order information. Such information also can	• The entity's computer system maintains a transaction history for each service requested and related transaction. • Upon completion of a transaction, the entity's	• The entity's computer system maintains a transaction history for all trades requested and related transaction. One year's transaction history can be viewed online.

Transaction Integrity - The entity maintains effective controls to provide reasonable assurance that customer's transactions using electronic commerce are completed and billed as agreed.			
Criteria	**Illustrative Disclosures for Retail Goods and Non-financial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
	be accessed by customer name and dates of ordering, shipping or billing. • The entity maintains this identifier and detailed order records that enable customers to contact the entity about details of orders for at least 90 days from order fulfillment. • Order history information is maintained for 6 months from the date of shipment and is available for immediate access by customer service representatives. After 6 months, this information is maintained in a form that can be accessed by customer service representatives within 3 days.	computer system issues a unique identifier (e.g., confirmation number) confirming that the transaction has been processed successfully, and displays the number to the customer together with the date and time of the transaction. Each transaction can be accessed by customer name or account number or date of transaction. • All transactions are also recorded on the customer statement that can be accessed by the customer. • Two years of customer transaction history is available to the entity to make inquiries and answer any client questions.	• Upon completion of a transaction, the entity's computer system issues a unique identifier (e.g., confirmation number) confirming that the transaction has been processed successfully, and displays the number to the customer together with the date and time of the transaction. Each transaction can be accessed by customer name or account number or date of transaction. • We mail out monthly statements for each month in which your account shows activity, and quarterly statements for inactive accounts. • Two years of customer transaction history is available to the entity to make inquiries and answer any client questions.
Monitoring			

Transaction Integrity - The entity maintains effective controls to provide reasonable assurance that customer's transactions using electronic commerce are completed and billed as agreed.			
Criteria	**Illustrative Disclosures for Retail Goods and Non-financial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
5. The entity maintains monitoring procedures that provide reasonable assurance of the following: • Its business practice disclosures on its Web site remain current. • Its transaction integrity controls remain effective. • Reports of noncompliance are promptly addressed and corrective measures taken.	• Management regularly receives and reviews information that permits monitoring of business disclosures and transaction integrity (such as complaint rates, return rates, customer surveys, warranty and replacement rates, etc.). • Non-compliance situations are corrected when discovered and remedial actions taken are closely monitored for 30 days to prevent recurrence.	• Management regularly receives and reviews information that permits monitoring of business disclosures and transaction integrity (such as transaction rejected reports, complaint rates, customer surveys etc.). • Non-compliance situations are corrected when discovered and remedial actions taken are closely monitored for 30 days to prevent recurrence.	• Management regularly receives and reviews information that permits monitoring of business disclosures and transaction integrity (such as transaction rejected reports, complaint rates, customer surveys etc.). • Non-compliance situations are corrected when discovered and remedial actions taken are closely monitored for 30 days to prevent recurrence.
Control environment			
6. The entity has a control environment that is generally conducive to reliable business practice disclosures on its Web site and effective controls over electronic commerce transaction integrity.	• Management has a strong commitment to customer satisfaction and effective controls as evidenced by maintaining a strong "tone at the top," hiring and developing competent personnel, periodically emphasizing the importance and responsibilities for	• Management has a strong commitment to customer satisfaction and effective controls as evidenced by maintaining a strong "tone at the top," hiring and developing competent personnel, periodically emphasizing the importance and responsibilities for	• Management has a strong commitment to customer satisfaction and effective controls as evidenced by maintaining a strong "tone at the top," hiring and developing competent personnel, periodically emphasizing the importance and responsibilities for

Transaction Integrity - The entity maintains effective controls to provide reasonable assurance that customer's transactions using electronic commerce are completed and billed as agreed.			
Criteria	**Illustrative Disclosures for Retail Goods and Non-financial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
	sound business practices and effective control, and supervising and monitoring business activities and control procedures.	sound business practices and effective control, and supervising and monitoring business activities and control procedures.	sound business practices and effective control, and supervising and monitoring business activities and control procedures.

Information Protection – The entity maintains effective controls to provide reasonable assurance that private customer information[3] obtained as a result of electronic commerce is protected from uses not related to the entity's business.			
Criteria	**Illustrative Controls for Retail Goods and Other Nonfinancial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
Transmission of private customer information 1. The entity maintains controls to protect transmissions of private customer information over the Internet from unintended recipients.	• Private customer information is protected during transmission by using encryption technology (Secure Sockets Layer (SSL) technology). The customer has the option of calling the entity's 800 number to provide his or her name, address, and credit card information to protect transmission of this information over the Internet. • The entity has registered its Domain Name and Internet IP address to protect its Internet identity. The address is unique and no more than one company can have the same address.	• Private customer information is protected during transmission by using 128-bit encryption technology (Secure Sockets Layer (SSL) technology). • The entity has registered its Domain Name and Internet IP address to protect its Internet identity. The address is unique and no more than one company can have the same address. • The entity's Web page has a digital certificate, which can be checked using features in a standard Web browser. • The entity's Webmaster updates the site and reviews and tests key Web pages at	• Private customer information is protected during transmission by using 128-encryption technology (Secure Sockets Layer (SSL) technology). • The entity has registered its Domain Name and Internet IP address to protect its Internet identity. The address is unique and no more than one company can have the same address. • The entity's Web page has a digital certificate, which can be checked using features in a standard Web browser. • The entity's Webmaster updates the site and reviews and tests key Web pages at

3 Private customer information includes personal identification information for the customer or his or her family (name, address, telephone number, social security or other government identification numbers, employer, credit card numbers, etc.), personal or family financial information, personal or family medical information, employment history, history of purchases or other transactions, credit records and similar information.

Information Protection – The entity maintains effective controls to provide reasonable assurance that private customer information[3] obtained as a result of electronic commerce is protected from uses not related to the entity's business.			
Criteria	**Illustrative Controls for Retail Goods and Other Nonfinancial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
	• The entity's Web page has a digital certificate, which can be checked using features in a standard Web browser. • The entity's Webmaster updates the site and reviews and tests key Web pages at least daily to ensure that improper content or links have not been added. • The entity provides guidance (e.g., Security FAQs) on its Web site outlining the customers' responsibilities to ensure customer information is transmitted securely.	least daily to ensure that improper content or links have not been added. • The entity provides guidance (e.g., Security FAQs) on its Web site outlining the customers' responsibilities to ensure customer information is transmitted securely.	least daily to ensure that improper content or links have not been added. • The entity provides guidance (e.g., Security FAQs) on its Web site outlining the customers' responsibilities to ensure customer information is transmitted securely.
Protection and use of private customer information The entity maintains controls to protect private customer information obtained as a result of electronic commerce and retained in its system from outsiders.			

Information Protection – The entity maintains effective controls to provide reasonable assurance that private customer information[3] obtained as a result of electronic commerce is protected from uses not related to the entity's business.			
Criteria	**Illustrative Controls for Retail Goods and Other Nonfinancial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
• Systems that retain private customer information obtained as a result of electronic commerce are protected from unauthorized outside access	• A recognized commercial firewall is used. It is updated monthly and is tested periodically for susceptibility to security weaknesses. • All private customer information is stored in directories defined with access control rules to prevent unauthorized access.	• A recognized commercial firewall is used. It is updated monthly and is tested periodically for susceptibility to security weaknesses. • Edit checks exist on all Web page input screens to disable unauthorized data that could trigger the unauthorized processing execution of system programs on the Web Server. • All private customer information is stored in directories defined with access control rules to prevent unauthorized access. • Directory browsing has been disabled on the Web Server to prevent outsiders from browsing a list of files (especially if no default index file has been defined).	• A recognized commercial firewall is used. It is updated monthly and is tested periodically for susceptibility to security weaknesses. • All private customer information is stored in directories defined with access control rules to prevent unauthorized access. • Edit checks exist on all Web page input screens to ignore unauthorized data that could trigger the unauthorized processing execution of system programs on the Web Server.
• Customers entering	• All system access from	• All access to customer	• All access to customer

Information Protection – The entity maintains effective controls to provide reasonable assurance that private customer information[3] obtained as a result of electronic commerce is protected from uses not related to the entity's business.			
Criteria	**Illustrative Controls for Retail Goods and Other Nonfinancial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
through the Web page cannot access other customers' private information.	outside the entity, other than for customary electronic commerce transactions through the Web page, (through the Internet, dial up, or other connections) is restricted by one-time passwords and/or smart cards.	accounts is restricted to the customer through the use of a unique digital certificate associated with each customer. • Customer sessions between the browser and electronic commerce systems are protected to avoid other users from hijacking a customer's session (e.g., use of unique digital certificates or cookies checking for random unique identifiers before the start of each session). • All system access from outside the entity, other than for customary electronic commerce transactions through the Web page, (through the Internet, dial up, or other connections) is restricted by authentication systems using one-time passwords.	accounts is restricted to the customer through the use of a unique user ID and secret password. • Customer sessions between the browser and the electronic commerce systems are protected to avoid other users from hijacking a customer's session (e.g., use of unique digital certificates or cookies checking for random unique identifiers before the start of each session). • All system access from outside the entity, other than for customary electronic commerce transactions through the Web page, (through the Internet, dial up, or other connections) is restricted by authentication systems using one-time passwords.
• Private customer	• Policy restricts the entity	• Policy restricts the entity	• Policy restricts the entity

Information Protection – The entity maintains effective controls to provide reasonable assurance that private customer information[3] obtained as a result of electronic commerce is protected from uses not related to the entity's business.			
Criteria	**Illustrative Controls for Retail Goods and Other Nonfinancial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
information obtained as a result of electronic commerce is not intentionally disclosed to parties not related to the entity's business unless (1) customers are clearly notified prior to their providing such information or (2) customer permission is obtained after they have provided such information.	staff from disclosing private customer information to any third party without the express consent of the customer or as otherwise provided by law.	staff from disclosing private customer information to any third party without the express consent of the customer or as otherwise provided by law.	staff from disclosing private customer information to any third party without the express consent of the customer or as otherwise provided by law.
• Private customer information obtained as a result of electronic commerce is used by employees only in ways associated with the entity's business	• All private customer information is restricted to only authorized persons within the entity and protected through effective authentication systems and/or encryption technology. • The entity has policies and monitoring procedures to ensure that only certain employees can access private customer	• All private customer information is restricted to only authorized persons within the entity and protected through effective authentication systems and/or encryption technology. • The entity has policies and monitoring procedures to ensure that only certain employees can access private customer	• All private customer information is restricted to only authorized persons within the entity and protected through effective authentication systems and/or encryption technology. • The entity has policies and monitoring procedures to ensure that only certain employees can access private customer

Information Protection – The entity maintains effective controls to provide reasonable assurance that private customer information[3] obtained as a result of electronic commerce is protected from uses not related to the entity's business.			
Criteria	**Illustrative Controls for Retail Goods and Other Nonfinancial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
	information. These policies also set forth ways that customer information can and cannot be used. Policy enforcements are made possible through conditions of employment statement.	information. These policies also set forth ways that customer information can and cannot be used. Policy enforcements are made possible through conditions of employment statement.	information. These policies also set forth ways that customer information can and cannot be used. Policy enforcements are made possible through conditions of employment statement.
Protection of customers' computers and files 2. The entity maintains controls to protect against its unauthorized access to customer's computers and its unauthorized modification of customer's computer files:			
• Customer permission is obtained before storing, altering or copying information in the customer's computer or the customer is notified with an option to prevent such activities.	• The entity requests the customer's permission before it intentionally stores, alters or copies information (such as cookies and other similar files) in the customer's computer. • The entity requests the	• The entity requests the customer's permission before it intentionally stores, alters or copies information (such as cookies and other similar files) in the customer's computer. • The entity requests the	• The entity requests the customer's permission before it intentionally stores, alters or copies information (such as cookies and other similar files) in the customer's computer. • The entity requests the

Information Protection – The entity maintains effective controls to provide reasonable assurance that private customer information[3] obtained as a result of electronic commerce is protected from uses not related to the entity's business.			
Criteria	**Illustrative Controls for Retail Goods and Other Nonfinancial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
	customer's permission before it performs any diagnostic or inventory on the customer's computer.	customer's permission before it performs any diagnostic or inventory on the customer's computer.	customer's permission before it performs any diagnostic or inventory on the customer's computer.
• Transmission of malicious computer code to customers is prevented	• The entity maintains antivirus software on its Web site, updates its virus signatures at least monthly, and takes reasonable precautions to protect both its systems and the customer's computer from viruses during the electronic commerce session. • The entity implements programming standards and conducts software testing to ensure Web pages using active content technologies (e.g., Java applets, Active X, JavaScripts) are not susceptible to security weaknesses.	• The entity maintains antivirus software on its Web site, updates its virus signatures at least monthly, and takes reasonable precautions to protect both its systems and the customer's computer from viruses during the electronic commerce session. • The entity implements programming standards and conducts software testing to ensure Web pages using active content technologies (e.g., Java applets, Active X, JavaScripts) are not susceptible to security weaknesses.	• The entity maintains antivirus software on its Web site, updates its virus signatures at least monthly, and takes reasonable precautions to protect both its systems and the customer's computer from viruses during the electronic commerce session. • The entity implements programming standards and conducts software testing to ensure Web pages using active content technologies (e.g., Java applets, Active X, JavaScripts) are not susceptible to security weaknesses.

Information Protection – The entity maintains effective controls to provide reasonable assurance that private customer information[3] obtained as a result of electronic commerce is protected from uses not related to the entity's business.			
Criteria	**Illustrative Controls for Retail Goods and Other Nonfinancial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
Monitoring 3. The entity maintains monitoring procedures that provide reasonable assurance regarding the following:			
• Its information protection controls remain effective.	• Management receives and reviews information that permits monitoring of information protection (such as attempts to bypass security controls, security violations, firewall and antivirus updates, virus incident reports, version release number of currently installed security and encryption software and most recent version release number of software from the software vendor, and actions taken to correct published security weaknesses).	• Management receives and reviews information that permits monitoring of information protection controls (such as attempts to bypass security controls, security violations, firewall and antivirus updates, virus incident reports, version release number of currently installed security and encryption software and most recent version release number of software from the software vendor, and actions taken to correct published security weaknesses).	• Management receives and reviews information that permits monitoring of information protection controls (such as attempts to bypass security controls, security violations, firewall and antivirus updates, virus incident reports, version release number of currently installed security and encryption software and most recent version release number of software from the software vendor, and actions taken to correct published security weaknesses).
• Reports of non-	• Non-compliance situations	• Non-compliance situations	• Non-compliance situations

Information Protection – The entity maintains effective controls to provide reasonable assurance that private customer information[3] obtained as a result of electronic commerce is protected from uses not related to the entity's business.			
Criteria	**Illustrative Controls for Retail Goods and Other Nonfinancial Services**	**Illustrative Controls for Online Banking**	**Illustrative Controls for Online Securities Trading**
compliance are promptly addressed and corrective measures taken.	are corrected when discovered and remedial actions taken are closely monitored for 30 days to prevent recurrence.	are corrected when discovered and remedial actions taken are closely monitored for 30 days to prevent recurrence.	are corrected when discovered and remedial actions taken are closely monitored for 30 days to prevent recurrence.
Control environment			
4. The entity has a control environment that is generally conducive to effective controls over protection of private customer information.	• Management has a strong commitment to customer satisfaction and effective controls as evidenced by maintaining a strong "tone at the top," hiring and developing competent personnel, periodically emphasizing the importance and responsibilities for sound business practices and effective control, and supervising business activities and control procedures.	• Management has a strong commitment to customer satisfaction and effective controls as evidenced by maintaining a strong "tone at the top," hiring and developing competent personnel, periodically emphasizing the importance and responsibilities for sound business practices and effective control, and supervising and monitoring business activities and control procedures.	• Management has a strong commitment to customer satisfaction and effective controls as evidenced by maintaining a strong "tone at the top," hiring and developing competent personnel, periodically emphasizing the importance and responsibilities for sound business practices and effective control, and supervising and monitoring business activities and control procedures.

Appendix A
Illustrative Examples of Practitioner Reports

Illustration No. 1 for Use in the United States
Independent Accountant's Report

To The Management of ABC Company, Inc.:

We have examined the assertion **[hot link to management's assertion]** by the management of ABC Company, Inc. (ABC) regarding the disclosure of its electronic commerce business practices on its Web site and the effectiveness of its controls over transaction integrity and information protection for electronic commerce (at WWW.ABC.COM) during the period August 1, 1998 through October 31, 1998.

These electronic commerce disclosures and controls are the responsibility of ABC Company's management. Our responsibility is to express an opinion on management's assertions with regards to the AICPA/CICA *WebTrust* Criteria **[hot link]** based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of ABC Company's electronic commerce business practices and its controls over the processing of electronic commerce transactions and the protection of related private customer information, (2) selectively testing transactions executed in accordance with disclosed business practices, (3) testing and evaluating the operating effectiveness of the controls, and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time, such as to accommodate dates in the year 2000, may alter the validity of such conclusions.

In our opinion, during the period August 1, 1998 through October 31, 1998 ABC Company, in all material respects:

- disclosed its business practices for electronic commerce transactions and executed transactions in accordance with its disclosed business practices,
- maintained effective controls to provide reasonable assurance that customers' orders placed using electronic commerce were completed and billed as agreed, and
- maintained effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce was protected from uses not related to ABC's business

based on the AICPA/CICA *WebTrust* Criteria.

The CPA *WebTrust* seal of assurance on ABC's Web site for electronic commerce constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

This report does not include any representation as to the quality of ABC's goods or services nor their suitability for any customer's intended purpose.

X, Y & Z (name of CPA firm)
Certified Public Accountants
City, State
November 4, 1998 (date of report)

ILLUSTRATION NO. 2 FOR USE IN CANADA

Auditor's Report

To The Management of ABC Company, Inc.:

We have audited ABC Company's disclosure of its electronic commerce business practices on its Web site and the effectiveness of its controls over transaction integrity and information protection for electronic commerce (at WWW.ABC.COM) during the period August 1, 1998 through October 31, 1998. These electronic commerce disclosures and controls are the responsibility of ABC Company's management. Our responsibility is to express an opinion on the conformity of those disclosures and controls with the AICPA/CICA *WebTrust* Criteria **[hot link]** based on our audit.

We conducted our audit in accordance with standards for assurance engagements established by the Canadian Institute of Chartered Accountants. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of ABC Company's electronic commerce business practices and its controls over the processing of electronic commerce transactions and the protection of related private customer information, (2) selectively testing transactions executed in accordance with disclosed business practices, (3) testing and evaluating the operating effectiveness of the controls, and (4) performing such other procedures as we considered necessary in the circumstances.

In our opinion, during the period August 1, 1998 through October 31, 1998, ABC Company, in all material respects:

- disclosed its business practices for electronic commerce transactions and executed transactions in accordance with its disclosed business practices,
- maintained effective controls to provide reasonable assurance that customers' orders placed using electronic commerce were completed and billed as agreed, and
- maintained effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce was protected from uses not related to ABC Company's business

in accordance with the AICPA/CICA *WebTrust* Criteria.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time, such as to accommodate dates in the year 2000, may alter the validity of such conclusions.

The CA *WebTrust* seal of assurance on ABC's Web site for electronic commerce constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

This report does not include any representation as to the quality of ABC's goods or services nor their suitability for any customer's intended purpose.

X, Y & Z (name of CA firm) — City, Province
Chartered Accountants — November 4, 1998 (date of report)

Appendix B
WebTrust[SM] Self-Assessment Questionnaire
Version 1.1 -– February 1, 1999

This questionnaire is for use by electronic commerce service providers in documenting their electronic commerce business practices disclosures and related controls and in documenting a basis for their assertion or representation that "on its Web site at www.___.____ during the period _____, 199__ through _____, 199__ the entity:

- Disclosed its business practices for electronic commerce transactions and executed transactions in accordance with its disclosed business practices,
- Maintained effective controls to provide reasonable assurance that customers' transactions processed using electronic commerce over the web were completed and billed as agreed, and
- Maintained effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce was protected from uses not related to its business

Based on the AICPA/CICA *WebTrust*[sm] Criteria."

Entity Name _____ Entity Location _____
Web Site URL _____ Server Location _____
Period Covered: From _____ Through _____
Date Prepared _____ Prepared By _____

I. General Information

A. Electronic Commerce Activities to Be Covered

1. Describe the entity's electronic commerce activities that are asserted/represented to meet the *WebTrust* Principles and Criteria.
    a) What goods / services are being sold / provided?
    b) Who is the typical customer?
    c) What is the typical form of payment?
2. What is the Web site URL?
3. Who is responsible for controlling these activities and what is their organization's reporting relationship to the entity's management?
4. How long has the entity been selling such goods and services through this form of electronic commerce?
5. If the electronic commerce activities have changed in the last 90 days, describe the nature of such changes and when each change occurred.

B. Information Systems Used to Support Electronic Commerce Activities

1. Web Site or Other Customer Interface Systems
    a) Description
    b) Who, in this entity, is responsible
    c) Describe any portion of these systems that is outsourced to third parties
    d) Describe the frequency and nature of changes to Web site and customer interface systems
2. Telecommunications & Network Systems
    a) Description
    b) Who, in this entity, is responsible
    c) Describe any portion of these systems that is outsourced to third parties
    d) Describe the frequency and nature of changes to telecommunications and network systems

3. Other Supporting Systems and Technology

   a) Description

   b) Who, in this entity, is responsible

   c) Describe any portion of these systems that is outsourced to third parties

   d) Describe the frequency and nature of changes to such systems and technology

C. Control Environment

1. Describe the factors in the entity's organization the contribute to a control environment that is generally conducive to reliable business practice disclosures on its Web site and effective controls over electronic commerce transaction integrity and the protection of related private customer information. Such factors might include, but not be limited to:

   a) Management's "tone at the top."

   b) Hiring, development, and retention of competent personnel.

   c) Emphasizing the importance and responsibilities for sound business practices and effective control.

   d) Supervising business activities and control procedures.

   e) Employing a suitable internal auditing function that periodically audits matters related to the entity's electronic commerce activities.

   f) Other factors.

II. Business Practice Disclosures

Principle - ***The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed practices.***

A. Description of Business Practices

1. Describe the entity's business practices and how such practices are disclosed to customers for each of the following:

   a) Descriptive information about the nature of the goods that will be shipped or the services that will be provided, including the following:

      (1) Condition of goods (i.e., whether they are new, used, or reconditioned).

      (2) Description of services (or service contract).

      (3) Sources of information (i.e., where it was obtained and how it was compiled).

      (4) Other relevant descriptive information.

   b) The terms and conditions by which electronic commerce transactions are conducted

      (1) Time frame for completion of transactions (transactions means fulfillment of orders where goods are being sold and delivery of service where a service is being provided).

      (2) Time frame and process for informing customers of exceptions to normal processing of orders or services requests (e.g., backorders or other order exceptions) and available customer options.

      (3) Normal method of delivery, including customer options, where applicable.

      (4) Payment terms, including customer options, if any.

      (5) Electronic settlement practices and related charges to customers.

      (6) How the customer may cancel recurring charges, if any.

      (7) Product return policies and/or limited liability, where applicable.

      (8) Other relevant terms and conditions, if any.

   c) Where on its Web site (and/or in information provided with the product) customers can obtain warranty, service, and support related to the goods and services purchased on the Web site.

   d) Information to enable customers to file claims, ask questions and register complaints, including, but not limited to, the following:

(1) Street address (not a post office box or e-mail address).

(2) Telephone number (a number to reach an employee on a reasonably timely basis and not only a voice mail system or message machine).

(3) Days and hours of operation.

(4) If there are several offices or branches, the same information for the principal office.

(5) Other relevant information for customers.

2. Describe who is responsible for controlling these activities.

3. Has the entity changed its business practices or the related disclosures in the last 90 days?

   a) If so, describe the nature of such changes and when each change occurred.

B. Where there are local, national, or other laws or requirements affecting business terms and conditions (e.g., customer rights and "lemon laws"):

1. Describe the entity's policies and procedures to provide reasonable assurance that it complies with such laws and requirements.

2. Where required by such laws and requirements, describe how appropriate disclosures provided to the customer.

C. Describe the entity's process for monitoring customer claims and complaints and for identifying patterns of claims and complaints that are not being satisfactorily addressed.

D. Describe the processes management uses to monitor the continuing effectiveness of its disclosure of business practices to provide reasonable assurance that:

1. The electronic commerce transactions it executes are in accordance with its disclosed business practices.

2. Its business practice disclosures on its Web site remain current and continue to meet the *WebTrust* Criteria.

3. Reports of noncompliance are promptly addressed and corrective measures taken.

E. Self-Assessment Questions (Yes / No / Not Applicable)

1. Does the entity disclose descriptive information about the nature of the goods that will be shipped or the services that will be provided, including, but not limited to, the following:

    a) Condition of goods (i.e., whether they are new, used, or reconditioned)?

    b) Description of services (or service contract)?

    c) Sources of information (i.e., where it was obtained and how it was compiled)?

2. Does the entity disclose the time frame for completion of transactions (transactions means fulfillment of orders where goods are being sold and delivery of service where a service is provided)?fulfillment of orders for goods and services?

3. Does the entity disclose the time frame and process for informing customers of exceptions to normal processing of orders or service requests (e.g., backorder or other order exceptions) and the available customer options?

4. Does the entity disclose its normal method of delivery and customer options, if any?

5. Does the entity disclose its payment terms and customer options, if any?

6. Does the entity disclose its electronic settlement practices and related charges to customers?

7. Does the entity disclose how the customer may cancel recurring charges, if any?

8. Does the entity disclose its return policies (or instances of limited liability, as applicable) or that there are no return practices?

9. Does the entity disclose descriptive information about the nature of the goods that will be shipped or the services that will be provided, including, but not limited to, the following:

    a) Condition of goods (i.e., whether they are new, used, or reconditioned)?

    b) Description of services (or service contract)?

    c) Sources of information (i.e., where it was obtained and how it was compiled)?

10. Does the entity disclose (on its Web site and/or in information provided with the product) where customers can obtain warranty, service and support related to the goods and services purchased on its Web site?

11. Does the entity disclose information to enable customers to file claims, ask questions and register complaints, including:

    a) Street address (not a post office box or e-mail address)?

    b) Telephone number (a number to reach an employee on a reasonably timely basis and not only a voice mail system or message machine)?

    c) Days and hours of operation?

    d) If there are several offices or branches, is the same information disclosed for the principal office?

III. Transaction Integrity Controls

Principle - ***The entity maintains effective controls to provide reasonable assurance that customer's orders placed using electronic commerce are completed and billed as agreed.***

A. Description of steps taken to ensure the integrity of electronic commerce transactions

1. Describe the controls maintained by the entity to ensure the integrity of electronic commerce transactions:

    a) How the entity provides reasonable assurance that:

        (1) Each request for transaction is checked for accuracy and completeness.

        (2) Positive acknowledgment is received from the customer before the transaction is processed.

    b) How the entity provides reasonable assurance that:

        (1) The correct goods are shipped in the correct quantities in the time frame agreed.

        (2) Services and information are provided to the customer as agreed to in the transaction.

        (3) Transaction exceptions (e.g., Back orders and other exceptions) are promptly communicated to the customer.

    c) How the entity provides reasonable assurance that:

(1) Sales prices and all other costs/fees are displayed for the customer before requesting acknowledgment of the transaction.

(2) Transactions are billed and electronically settled as agreed.

(3) Billing or settlement errors are promptly corrected.

d) How entity maintains controls that allow for subsequent follow-up of orders.

2. Describe who is responsible for controlling these activities.

3. Has the entity changed its controls over transaction integrity in the last 90 days?

a) If controls over transaction integrity have changed, describe the nature of such changes and when each change occurred.

B. Describe the processes management uses to monitor the continuing effectiveness of its controls over transaction integrity to provide reasonable assurance that:

1. Its transaction integrity controls remain effective.

2. Its transaction integrity controls continue to meet the *WebTrust* Criteria.

3. Reports of noncompliance are promptly addressed and corrective measures taken.

C. Self-Assessment Questions (Yes / No / Not Applicable)

1. Does the entity maintain controls to provide reasonable assurance that:

a) Each request or transaction is checked for accuracy and completeness?

b) Positive acknowledgment is received from the customer before the transaction is processed?

2. Does the entity maintain controls to provide reasonable assurance that:

a) The correct goods are shipped in the correct quantities in the time frame agreed?

b) Services and information are provided to the customer as agreed to in the transaction?

c) Transaction exceptions (e.g., bBack orders and other exceptions) are promptly communicated to the customer?

3. Does the entity maintain controls to provide reasonable assurance that:

   a) Sales prices and all other costs/fees are displayed for the customer before requesting acknowledgment of the transaction?

   b) Transactions are billed and electronically settled as agreed?

   c) Billing or settlement errors are promptly corrected?

4. Does the entity maintain controls that allow for subsequent follow-up of orders?

5. Does the entity maintains monitoring procedures that provide reasonable assurance that:

   a) Its business practice disclosures on its Web site remain current?

   b) Its transaction integrity controls remain effective?

   c) Reports of noncompliance are promptly addressed and corrective measures taken?

6. Does the entity have a control environment that is generally conducive to reliable business practice disclosures on its Web site and effective controls over electronic commerce transaction integrity?

IV. Information Protection Controls

Principle - ***The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce is protected from uses not related to the entity's business.***
In this context, private customer information includes personal identification information for the customer or his or her family (name, address, telephone number, social security or other government identification numbers, employer, credit card numbers, etc.), personal or family financial information, personal or family medical information, employment history, history of purchases or other transactions, credit records or similar information.

A. Description of steps taken to ensure the protection of private customer information.

1. Describe the controls maintained by the entity to protect transmissions of private customer information over the Internet from unintended recipients.

2. Describe the controls maintained by the entity to protect private customer information obtained as a result of electronic commerce and retained in its system from outsiders:

   a) How systems that retain private customer information obtained as a result of electronic commerce are protected from unauthorized outside access.

   b) How the entity ensures that customers entering through the Web page cannot access other customers' private information (i.e., they can only perform inquiries, execute transactions, and obtain information about their own transactions).

   c) How private customer information obtained as a result of electronic commerce is protected from intentional disclosure to parties not related to the entity's business unless:

      (1) Customers are clearly notified prior to their providing such information, or

      (2) Customer permission is obtained after they have provided such information.

   d) How the entity ensures that private customer information obtained as a result of electronic commerce is used by employees only in ways associated with the entity's business.

3. Describe the controls maintained by the entity to protect against its unauthorized access to customer's computers and its unauthorized modification of customer's computer files:

   a) How the entity ensures that customer permission is obtained before storing, altering or copying information in the customer's computer (including the use of "cookies" stored on the customer's computer system) or that the customer is notified with an option to prevent such activities.

b) How the entity ensures that transmission of malicious computer code (e.g., viruses) to customers is prevented.

4. Who is responsible for controlling these activities?

5. Has the entity changed its controls over information protection in the last 90 days?

   a) If so, describe the nature of such changes and when each change occurred.

B. Describe the processes management uses to monitor the continuing effectiveness of its controls over information protection to provide reasonable assurance that:

1. Its information protection controls remain effective.

2. Its transaction integrity controls continue to meet the *WebTrust* Criteria.

3. Reports of noncompliance are promptly addressed and corrective measures taken.

C. Self-Assessment Questions (Yes / No / Not Applicable)

1. Does the entity maintain controls to protect transmissions of private customer information over the Internet from unintended recipients?

2. Does the entity maintain controls to protect private customer information obtained as a result of electronic commerce and retained in its system from outsiders:

   a) Are systems that retain private customer information obtained as a result of electronic commerce protected from unauthorized outside access?

   b) Are customers entering through the Web page restricted from accessing other customer' private information (i.e., a customer can only perform inquiries, execute transactions, and obtain information about their own transactions)?

   c) Is private customer information not intentionally disclosed to parties not related to the entity's business unless:

      (1) Customers are clearly notified prior to their providing such information, or

      (2) Customer permission is obtained after they have provided such information?

d) Is private customer information used by employees only in ways associated with the entity's business?

3. Does the entity maintain controls to protect against its unauthorized access to customer's computers and its unauthorized modification of customer's computer files:

   a) Customer permission is obtained before storing, altering or copying information in the customer's computer or the customer is notified with an option to prevent such activities?

      (1) Does this include obtaining permission or providing customer notification before using "cookies"?

   b) Transmission of malicious computer code (e.g., viruses) to customers is prevented?

4. Does the entity maintain monitoring procedures that provide reasonable assurance that:

   a) Its information protection controls remain effective?

   b) Reports of non-compliance are promptly addressed and corrective measures taken?

5. Does the entity have a control environment that is generally conducive to effective controls over protection of private customer information?

V. Change Management and CPA/CA Notification

A. Description of the Change Management Process

1. Describe the entity's controls over changes to its electronic commerce business practices, its transaction integrity controls, its information protection controls, and its electronic commerce systems and supporting technology, which are designed to provide reasonable assurance that:

   a) All such changes are approved by management.

   b) Changes in business practices are reflected in modified disclosures of such practices.

c) Changes in the manner in which electronic commerce transactions are executed are reflected in modified business practice disclosures.

d) Modified business practice disclosures continue to conform to the *WebTrust* Criteria.

e) Controls over transaction integrity and information protection continue to function effectively and to conform to the *WebTrust* Criteria.

B. Description of the Process to be Used to Notify CPA or CA of Changes

1. Describe the entity's policies and procedures to notify the CPA or CA *in advance* of making changes to its:

   a) Electronic commerce activities,

   b) Electronic commerce systems and supporting technology,

   c) Business practices and disclosures of business practices,

   d) Controls over transaction integrity,

   e) Controls over information protection,

   f) Monitoring procedures over the foregoing, and

   g) Control environment.

2. Who is responsible for notifying the CPA or CA of such changes?

3. Has the entity changed those controls, procedures, or responsibilities designed to provide reasonable assurance that the CPA or CA is notified of all relevant changes in the last 3 months?

   a) If so, describe such changes and when each was made.

VI. Other Matters

A. Describe below any other matters that would be relevant to the CPA or CA in evaluating the Web site's conformity with the *WebTrust* Criteria. Examples might include:

1. Significant changes in the entity's business or its organizational structure.

2. Significant problems in meeting demand for its goods and services, meeting its customer commitments or continuing its historical level of customer satisfaction (e.g., as might be evidenced by unusual levels of customer complaints).

3. Significant processing or controls problems with the entity's electronic commerce systems or supporting infrastructure.

4. Instances of fraud and breaches of transaction integrity, security and information protection controls involving:

   b) employees with electronic commerce responsibilities,

   c) contractors and others who provide services to the entity related to its electronic commerce activities,

   d) unauthorized third parties, or

   e) systems and supporting infrastructure used for executing electronic commerce transactions.

5. Significant changes in management and other key personnel with electronic commerce responsibilities.

6. Other relevant information.